VMware® vSphere 5.0

Guidance Documentation Supplement

Evaluation Assurance Level: EAL4+

DOCUMENT VERSION: 0.2

vmware®

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
United States of America

Phone: +1 (650) 475-5000
http://www.vmware.com

VMware Security Advisories, Certifications and Guides
http://www.vmware.com/security/

Prepared for VMware by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America
Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

List of Tables

Table of Figures

1 Introduction

The Target of Evaluation (TOE) is the vSphere 5.0. The TOE is a software-only system, which provides an environment for hosting multiple virtual machines (VMs) on industry standard x86-compatible hardware platforms and provides management of virtual machines.

1.1 Purpose

This document provides guidance on the secure installation of the TOE for the Common Criteria Evaluation Assurance Level (EAL) 4+ Evaluated Configuration. This document provides clarifications and changes to the VMware documentation and should be used as the guiding document for installation of the TOE in the Common Criteria evaluated configuration. The official VMware documentation should be referred to and followed only as directed within this guiding document.

Table 1 below lists the guidance documents relevant to the installation and configuration of the TOE.

Table 1 – TOE Guidance Documents

Document Name	Description
• vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0 • vSphere Upgrade, vSphere 5.0, ESXi 5.0, vCenter Server 5.0, vSphere Client 5.0	Includes steps for the basic initialization and setup of the TOE.

.

Document Name	Description
• vSphere Availability, ESXi 5.0, vCenter Server 5.0 • vCenter Server and Host Management, ESXi 5.0, vCenter Server 5.0 • vSphere Host Profiles, ESXi 5.0, vCenter Server 5.0 • vSphere Monitoring and Performance, vSphere 5.0, vCenter Server 5.0, ESXi 5.0 • vSphere Networking, ESXi 5.0.0, vCenter Server 5.0.0 • vSphere Resource Management, ESXi 5.0, vCenter Server 5.0 • vSphere Security, ESXi 5.0, vCenter Server 5.0 • vSphere Troubleshooting, ESXi 5.0, vCenter Server 5.0 • vSphere Virtual Machine Administration, ESXi 5.0, vCenter Server 5.0 **Additional Resources:** • VMware vSphere Basics, ESXi 5.0, vCenter Server 5.0 • VMware vSphere Examples and Scenarios, ESXi 5.0, vCenter Server 5.0 • vSphere Storage, ESXi 5.0, vCenter Server 5.0 • Command-Line Management in vSphere 5.0 for Service Console Users • Getting Started with vSphere Command-Line Interfaces.	Contains detailed steps for how to properly configure and maintain the TOE.

1.2 Target Audience

The audience for this document consists of the end-user, the VMware development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

1.3 Evaluated TOE Configuration

Figure 1 depicts the evaluation configuration of the TOE, and contains the following previously undefined acronyms:

- OS – Operating System
- VM – Virtual Machine
- VUM – VMware vCenter Update Manager

.

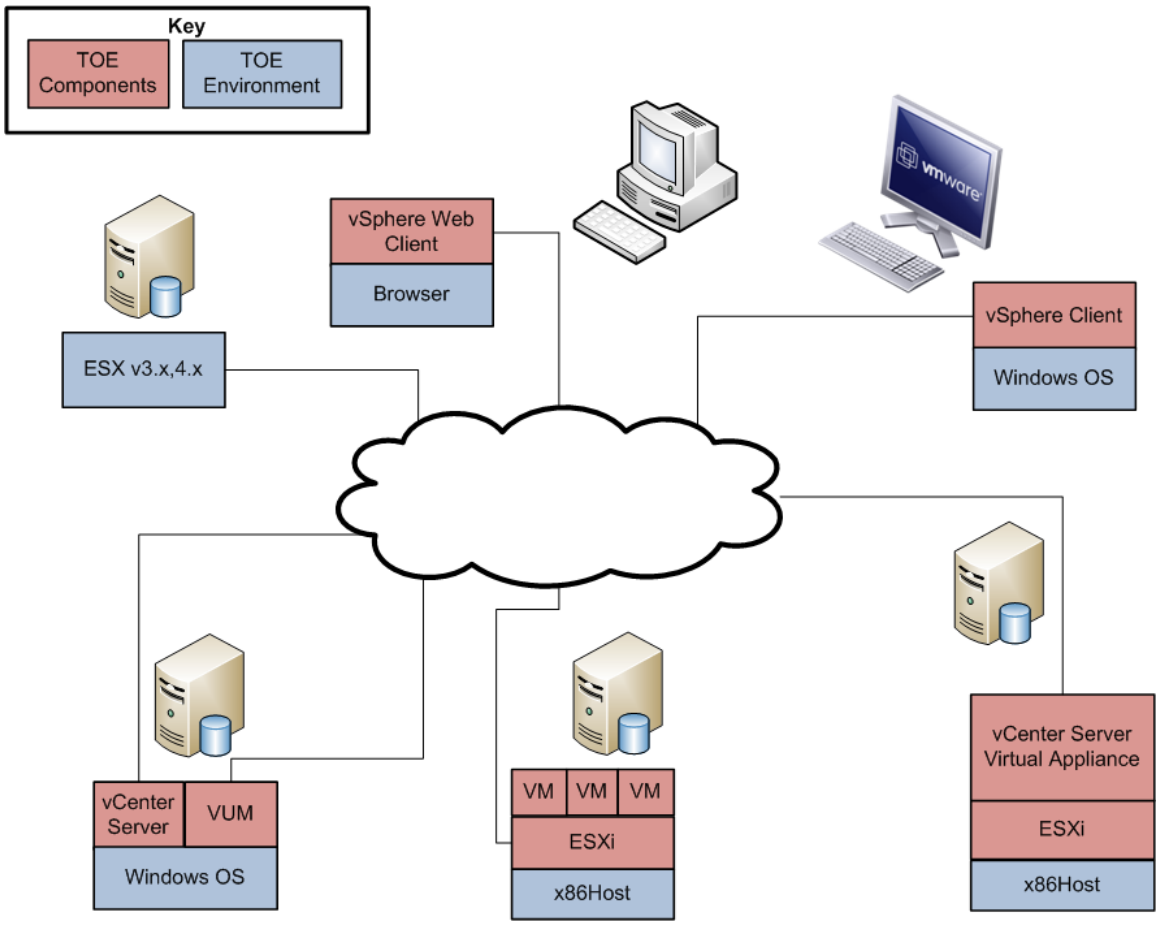

Figure 1 – Sample Deployment Configuration of the TOE

1.4 Assumptions

The writers of this document assume the following:

- Users are non-hostile, appropriately trained, and follow all user guidance.
- The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access. The vSphere Client component will only connect to the server via the protected management network.
- The administrator is familiar with and knowledgeable on the documents listed above in Table 1 – TOE Guidance Documents.

2 Installation Procedure

This section describes the installation procedure notes and changes.

2.1 Introduction

This section provides guidance for how to properly install and setup the vCenter Server and setup ESXi as documented in the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document, along with additions and changes to the instructions contained therein, in order to allow the administrator to properly install and setup the evaluated configuration of the TOE.

Before the administrator begins the installation and setup, he should make certain that he has all the necessary components. The components needed to install and setup the TOE are listed in section 2 "System Requirements" of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document.

The architecture of the evaluated configuration consists of the following components:

- ESXi 5.0
- vCenter Server Virtual 5.0
- vCenter Server Virtual Appliance 5.0
- vSphere Client 5.0
- vSphere Web Client on a supported web browser (Internet Explorer 8.0 or Firefox 3.6.3)

2.2 Secure Installation

Note: Throughout this section the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the documents listed in Table 1.

2.2.1 Phase 1 – Initial Preparation

The ESXi is a user-installable or OEM[1]-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, which provides the environment for multiple virtual machines to be hosted on one physical server. Virtual machines are the containers in which guest operating systems run. The OEM-Embedded version of ESXi is embedded as firmware on hardware, it is already installed by the hardware manufacturer and just needs to be setup by an administrator.

Sections 9 and 10 of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document list the prerequisite steps before installing the vCenter Server 5.0. Before beginning the install process for the vCenter Server 5.0, the administrator should ensure that he has the necessary system requirements and prerequisites needed for the vCenter Server 5.0. This information is provided in section 2 of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document.

It should be noted that when the vCenter Server 5.0 is downloaded via VMware's website, a SHA-1[2] hash is provided to the customer on the product download page. To confirm the downloaded TOE's integrity, a SHA-1 hash utility should be used to calculate a SHA-1 hash for the downloaded TOE. If the calculated SHA-1 hash matches the SHA-1 hash provided on VMware's website, the TOE downloaded correctly. Should the TOE fail the SHA-1 hash procedure, the customer should download the TOE & SHA-1 hash

[1] OEM Original Equipment Manufacturer
[2] Secure Hash Algorithm 1

again and re-check the TOE's integrity with the SHA-1 hash. If the failure persists, the customer should contact VMware customer support.

2.2.2 Phase 2 – Installation of the TOE

There are several options for installing the ESXi component of the TOE. Detailed steps for these options can be found in sections 3, 4, 5, and 6 of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document. Detailed steps for setting up the ESXi component of the TOE can be found in section 7 of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document. .

Detailed steps for installing the vCenter Server 5.0 component of the TOE can be found in section 11 of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document. Post-installation options for the vCenter Server 5.0 can be found in section 12 of the *vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0* document .

3 Administrative Guidance

This section provides guidance for how to properly step through the configuration and maintenance instructions documented in the *vSphere Security ESXi 5.0 vCenter Server 5.0* guide, along with additions and changes to the instructions contained therein, in order to allow the administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should follow all the guidance documentation that is listed in Table 1 to ensure the proper installation, configuration, and management of the TOE Security functions.

3.1 Clarifications

The following sections describe clarifications to the administrative guidance of the TOE.

3.1.1 ESXi 5.0 and vCenter Server 5.0 Passwords

This section provides guidance for how an authorized TOE user must create a password to be used for the VMware Service Console and vSphere Web Access interfaces.

An authorized TOE user must use an appropriately complex password to access the TOE. To adequately protect the TOE from unauthorized use, administrators are required to enforce a password policy that contains the following rules:

- the password must have a minimum password length of eight characters
- the password must contain at least one numeric character (from a set of 10)
- the password may also include non-alphanumeric characters (from a set of 32), and alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated)

On ESXi the password policy is enforced by the Pam Password Quality-Control module which is enabled by default. By default pam_passwdqc is configured as shown below.

```
pam_passwdqc.so retry=3 min=8,8,8,7,6
```

For vCenter Server, since passwords are generated and stored in the TOE Environment, Administrators must ensure that the Environment enforces this policy and that users abide by it.

For vCenter Server Virtual Appliance, password are generated and stored in the TOE Environment as well. Administrator must ensure that the Environment enforces the password policy and that users abide by it. During initial configuration of the vCenter Server Virtual Appliance, the default root password is pre configured and does not follow the password policy. Administrators are responsible to changing the default root password to follow the password policy during initial configuration.

3.1.2 Special Instructions for Creating New Users and Changing User Passwords

Since only password strength checking is enforced on the passwords generated by users operating with root privileges, care must be taken by TOE administrators to ensure that the password policy is correctly enforced. Administrators creating a new user account must ensure that they follow the password policy described above when setting the initial password set for new users, and that they require the users to change their passwords on first login. Administrators must not change their own passwords using root privileges.

3.1.3 Maintaining Supported Windows Operating System and Supported Database for vCenter

Because vCenter Server resides (runs on) a Windows based host operating system, it is especially critical to protect this host operating systems against vulnerabilities and attacks. The standard set of recommendations applies, as it would for any host operating system: install antivirus agents, spyware filters, intrusion detection systems, and any other security measures. Administrators must make sure to keep all security measures up-to-date, including the supported MS-Windows operating system and application of patches.

Administrators should consult Microsoft for Windows updates and patches and consult supported database vendors for database-specific updates and patches.

For host and guest Operating System compatibility user, administrators should see the VMware Compatibility Guide at:
http://www.vmware.com/resources/compatibility/search.php .

For VMware product compatibility, administrators should see the VMware Product Interoperability Matrix at:
http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?

3.1.4 Default Self-Signed Certificates

Client sessions with vCenter Server may be initiated from any vSphere API[3] client, such as vSphere Client and PowerCLI. By default, SSL[4] encryption protects this connection, but the default certificates generated at the time of install are not signed by a trusted certificate authority and, therefore, do not provide the authentication security one might need in a production environment.

These self-signed certificates are vulnerable to man-in-the-middle attacks, and clients receive a warning about them. If an administrator intends to use encrypted remote connections externally, he should consider purchasing a certificate from a trusted certificate authority or use his own security certificate for his SSL connections.

Self-signed certificates are automatically generated by vCenter Server during the installation process. The certificates should be treated as temporary signatures for initial installation purposes only.

Administrators should replace the default self-signed certificate with those from a trusted certification authority: either a commercial CA or a organizational CA.

For new certificate installations or existing certificate installations on vSphere, administrators should use the “vSphere Security ESXi 5.0 vCenter Server 5.0 Section 5 administrator guide.

Certificates are currently stored in C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\.

3.1.5 SSH[5]

ESXi has a standard SSH interface which SSH clients can connect to in order to execute command line functions securely. SSH is disabled by default, but should be enabled for secure command line operations. SSH can be enabled in the Direct Console User Interface. See the vSphere Security Guidance document, section “Use the Direct Console User Interface (DCUI) to Enable Access to the ESXi Shell” for

[3] Application Programming Interface
[4] Secure Sockets Layer
[5] Secure Shell

instructions on how to enable SSH. In addition, configure the timeout value for the ESXi Shell to be 15 minutes. The timeout setting is the number of minutes that can elapse before a user must log in after the ESXi Shell is enabled. After the timeout period, if the user has not logged in, the shell is disabled.

If the user is logged in when the timeout period elapses, their session will persist. However, the ESXi Shell will be disabled, preventing other users from logging in.

4 Acronyms and Terms

This section defines the acronyms and terms.

Table 2 – Acronyms and Terms

Acronym	Definition
API	Application Programming Interface
EAL	Evaluated Assurance Level
OEM	Original Equipment Manufacturer
OS	Operating System
SAN	Storage Area Network
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TOE	Target of Evaluation
VM	Virtual Machine
VUM	VMware Update Manager

.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com